Statement of James X. Dempsey
Executive Director
Center for Democracy & Technology[1]

before the
Senate Committee on Commerce, Science and Transportation

S. 2281, The VOIP Regulatory Freedom Act of 2004

June 16, 2004

Mr. Chairman, Senator Hollings, Members of the Committee, thank you for the opportunity to testify today on the question of what should be the regulatory framework for voice communication services that use the technologies and infrastructure of the Internet. We commend Senator Sununu for introducing S. 2281, and we commend you, Mr. Chairman, for calling this hearing and for opening this crucial debate.

As S. 2281 correctly posits, the Internet and applications like Voice over Internet Protocol (VOIP) services are different from traditional telecommunications services, so significantly different that they have not been and should not be regulated under the traditional regulatory framework for telecommunications. For reasons that are still valid today, the Internet and Internet applications were not included in the regulatory mandates of the Communications Assistance for Law Enforcement Act of 1994 (CALEA). After an in-depth factual inquiry in the early 1990s, Congress focused on specific problems law enforcement agencies were encountering in carrying out surveillance in the public

[1] The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values for the new digital communications media. Our core goals include enhancing privacy protections and preserving the open architecture of the Internet. Among other activities, CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies and associations interested in communications privacy and security issues.

switched telephone network (PSTN). With CALEA, Congress imposed design obligations on already heavily regulated telecommunications common carriers. Congress expressly excluded the Internet from those design mandates, because it was committed to the non-regulatory approach, because it found no problems on the Internet, and because it was uncertain of how surveillance mandates would translate to the Internet.

Consequently, the Federal Communications Commission has no authority to extend CALEA to the broadband Internet. Only Congress has that authority, and if Congress looks at the issues, conducting the same type of inquiry that it conducted a decade ago, we believe it will find that CALEA should not be extended to the Internet. As a threshold matter, there is no evidence that CALEA-type mandates are needed for the Internet. Service providers are already committed to cooperating. Moreover, the approach taken by the FCC in applying CALEA to the centralized PSTN – adopting detailed "punchlists" of surveillance features to be applied uniformly and ubiquitously -- is ill-suited to the decentralized architecture of the Internet and the innovative and diverse applications offered over it.

There is much of merit in S. 2281, and CDT supports its overall philosophy of treating the Internet differently for regulatory purposes, but we focus in our testimony here on the law enforcement issues. Clearly, the law enforcement and national security interests in being able to carry out electronic surveillance on all forms of communications are very important. However, the Internet today is not a haven for terrorists and drug dealers, and there is nothing in the Sununu bill that would make it so in the future. Tapping the Internet will be different than tapping the telephone system, but on balance it will be no harder, once law enforcement gets up to speed on the technology. If Congress

takes account of not only the law enforcement interests but also the other national interests in promoting innovation, maintaining American leadership of Internet technology development, expanding access, keeping costs down, enforcing competition, protecting privacy, and enhancing network security, it will conclude, as the Sununu bill does, that the regulatory framework of CALEA -- designed for the telephone network -- is ill-suited to the Internet and Internet applications.

I. CALEA Was Adopted for the PSTN

In the early 1990s, during the first Bush Administration and then in the Clinton Administration, the FBI began complaining that technological changes in the PSTN were interfering with law enforcement's ability to carry out wiretaps. The Justice Department initially asked Congress to enact legislation giving the Attorney General the power to set standards for all providers of electronic communications services. Congress balked at such a sweeping mandate. Instead, Congress insisted first and foremost on a factual inquiry into what exactly were the problems being encountered by law enforcement. Hearings were held. The General Accounting Office conducted two studies. The FBI surveyed its field offices twice. Industry and law enforcement convened action teams to study the concerns of law enforcement and possible solutions. At the end of the process, industry representatives agreed that new technologies were defeating law enforcement surveillance. Some of the problems had to do with features such as call forwarding and speed dialing. Others had to do with the transition to multiplexed lines and fiber optic cables. Yet others had to do with the lack of sufficient capacity on switches to

simultaneously accommodate a large number of intercepts.[2]

Based on this factual showing, and after further consultation and negotiation, Congress came forth with a bill that was fundamentally different from the one initially sought by the Justice Department. As adopted, CALEA did not give the Attorney General the power to issue standards for telecommunications networks. Instead, CALEA set forth four broad functional requirements, 47 USC §1002(a), and it gave industry the authority to adopt it own standards on how to achieve them, 47 USC §1006(a). If law enforcement was dissatisfied, it had to petition the FCC, 47 USC §1006(b), whose decisions were in turn subject to judicial review. Carriers were required to provide access to information only if it was "reasonably available" to them. 47 USC §1002(a)(2). Private networks were exempted, as were interconnection services. 47 USC §1002(b)(2). The legislation expressly said there was no obligation on service providers to decrypt communications scrambled by end users. 47 USC §1002(b)(3). Enforcement was placed in the courts, and Congress made it clear that no carrier would be found liable if compliance was not reasonable, nor would a carrier be liable if the information was available somewhere else in the network. 47 USC §1007. A separate rulemaking was authorized to establish capacity requirements. 47 USC §1003.

Most importantly, Congress chose to extend the design mandate only to those entities providing telecommunications services as common carriers. 47 USC §§1001(8); 1002(a). That is where the documented problems were. That is where there were clear solutions. Congress recognized that the PSTN was a relatively centralized, relatively monopolized industry. The switches for the PSTN were made by a handful of switch

---

[2] *Telecommunications Carrier Assistance to the Government*, H.R. Rep. 103-827(I) at 14-16 (Oct. 4, 1994).

manufacturers, who agreed that they had not built in easy intercept access points. The Congress focused its regulatory action on these telecommunications common carriers – entities already subject to a range of regulatory burdens.

On the other hand, Congress found that the Internet was not posing a problem. Moreover, Congress was reluctant to impose design mandates on such a diverse and rapidly changing medium.

At the time, the regulatory world was divided into two categories: telecommunications services carried over the public switched telephone network, and "information services," which Congress and the Federal Communications Commission used as shorthand for the Internet and the applications running over it (among other services). Accordingly, Congress limited CALEA to telecommunications common carriers and expressly excluded "information services" such as the Internet from CALEA obligations. The term "information services" was broadly defined to cover current and future advanced software and software-based electronic messaging services, including email, text, voice and video services. Narrowband Internet access and Internet applications like email fit squarely within the definition. As the broadband Internet has evolved, it continues to be outside the scope of telecommunications common carriage, and Internet-based telephony services, like all other Internet applications, fit squarely within the definition of information services.

The legislative history could not be clearer: The Committee Report states that CALEA obligations "do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America On-line or Mead Data, or Internet service providers." *Telecommunications Carrier Assistance to the*

Government, H.R. Rep. 103-827(I), at 23 (Oct. 4, 1994) ("*House Report*"). As the FBI Director testified, CALEA was "narrowly focused on where the vast majority of our problems exist -- the networks of common carriers, a segment of the industry which historically has been subject to regulation."[3]

When the Court of Appeals reviewed the FCC's CALEA implementation order, the Court noted, "CALEA does not cover 'information services' such as email and internet access." *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000). And the FCC found that information services "such as electronic mail providers and on-line service providers" are exempt from CALEA. *In the Matter of Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 FCC Rcd 7105, at ¶ 26 (1999).

II. The Internet is Already Tappable

As a legal matter, there is no impediment to tapping voice or data communications over the Internet. The Internet is already subject to the wiretap laws, which authorize courts to issue surveillance orders for all types of electronic communications. Furthermore, all providers of VOIP services are already under a legal obligation to cooperate with all court orders for interception. Under 18 USC § 2518(4), any service provider can be required under a wiretap order to provide "forthwith all information, facilities, and technical assistance necessary to accomplish the interception." (Similar authority compels the assistance of service providers in carrying out

[3] Testimony of Louis Freeh before the Joint Hearing of the Technology and Law Subcommittee of the Senate Judiciary Committee and the Civil and Constitutional Rights Subcommittee of the House Judiciary Committee, Mar. 18, 1994, available at http://www.eff.org/Privacy/Surveillance/CALEA/freeh_031894_hearing.testimony.

interceptions of signaling information under the pen register and trap and trace statute, 18 USC § 3124(a).)

Moreover, as a practical matter, the broadband technologies used for VOIP are already tappable at one or more points in the networks. Service providers are quite willing to work with law enforcement to satisfy interception orders quickly and fully when they receive them. The cable industry has already developed a standard for interception of voice communications offered by cable companies. Cisco, a major maker of Internet routing equipment, already offers an interception capability in its equipment. Companies like VeriSign are offering packet interception services.

Last year, only 12 of the 1,442 state and federal wiretap orders were issued for computer communications, and the FBI has not argued that it had difficulty implementing any of those 12 wiretaps. Indeed, out of all 1,442 authorized wiretaps, the "most active" was the interception of a DSL line in Minnesota, suggesting that law enforcement agencies can readily intercept broadband communications.[4]

III. CALEA Implementation in the PSTN Has Been Plagued by Problems

Even as applied to the relatively centralized PSTN, CALEA has not worked well. The FBI and DOJ admit as much in their petition to the FCC. Indeed, their petition is almost schizophrenic: the first half argues that the Internet should be brought within the regulatory scheme of CALEA while the second half lays out a litany of delays, confusion

[4] "Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications," issued April 30, 2004, available at http://www.uscourts.gov/wiretap03/contents.html.

and controversy under CALEA as applied to the PSTN.[5] The FBI states that the CALEA implementation process "is not working." Petition, at 38. It cites "problems and delays," *id.* at 53; a "seemingly endless cycle of extensions that have consistently plagued the CALEA compliance process," *id.* at 55; and more "problems and delays," *id.* It states that "carriers continue to express uncertainty," *id. at* 64*,* and that "a growing number of law enforcement agencies have increasingly expressed concern," *id.* at 68.

This record of disfunctionality is confirmed by a report by the Office of the Inspector General (OIG) of the U.S. Department of Justice, issued on April 7, 2004.[6] The OIG's biannual audit, mandated by CALEA, evaluates the progress of CALEA compliance, and finds broad problems. The report, for example, notes that costs of CALEA for the PSTN have been much higher than Congress anticipated. The report also shows that the FBI's insistence on it "punchlist" has caused enormous problems within the CALEA standards setting efforts of industry.

Simply put, CALEA has proven to be a flawed statute. As to why, there is probably enough blame to go around. One key factor is that, contrary to Congress' intent, the FBI exercised de facto power to impose specific design mandates on the PSTN. This came about as a result of the interplay between the law's safe harbor provision and the process for FCC review of standards. As industry tried to develop a standard to implement CALEA, the FBI issued detailed "requirements" documents defining very

---

[5] Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, FCC RM-10865 (filed Mar. 10, 2004).

[6] "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," available at http://www.usdoj.gov/oig/audit/FBI/0419/final.pdf.

precise features it wanted built into communications equipment and architectures. The FBI told carriers that it would challenge as deficient any standard that did not include all its stated "requirements." Carriers and their equipment manufacturers were eager to take advantage of CALEA's safe harbor provision, and incorporated many of the FBI's design features, even if they did not seem to be required by CALEA. Nevertheless, at the end of the day, the FBI challenged the industry standard as deficient before the FCC because it did not include each and every item. The FCC thereupon ordered the industry standard rewritten to conform to the FBI's "punchlist."

In this process, the FBI succeeded in imposing on industry surveillance features that went beyond even the capabilities of the traditional telephone system. For example, the FCC imposed at least $120 million in costs on industry to obtain one feature known as "dialed digit extraction," which requires local exchange carriers, after call set-up, to reach into the content of the communications and extract additional dialed numbers, such as the numbers called on a long distance calling card. The FBI could have obtained the information it wanted by going to the providers of long distance services, but it wanted to obtain the information more conveniently through the local phone system. But this solution was very expensive solution for carriers. Indeed, the FBI could have purchased the extraction devices itself and attached them as necessary, a solution that the FBI itself estimated would cost no more than $20 million a year, but instead the FBI insisted that all carriers install them on all switches. The FBI also successfully convinced the FCC to impose on industry millions in dollars of costs in order to provide separate identifying notices every time a party on a conference call joined, dropped off, or put the call on hold. In these and other ways, the FBI used CALEA to expand, rather than merely

preserve, its intercept capabilities as technology changed.

IV. Meeting Law Enforcement Needs in a Sensible Way

Clearly, a different approach is needed for the Internet. Government agencies should not expect that surveillance will be carried out on the Internet the same way it is carried out in the circuit-switched telephone network. The digital revolution has produced many means of communication and it is not reasonable to require that all of them identify calls and route traffic the same way that the telephone network does. Internet interception may be less convenient for law enforcement than PSTN interception; given the diversity of services, the information will come in different formats and law enforcement will have to work harder to determine what it is intercepting. In many cases, law enforcement agencies will have to decode call-identifying information themselves. In some situations, law enforcement will have to obtain call-identifying information from an entity other than the one from which it obtains content. In other ways, however, Internet surveillance will be easier, in that the digital nature of communications makes them easier to analyze, store, manipulate and transfer. And Internet surveillance will certainly be more fruitful, with no need for design mandates, as more and more information moves online.

Yet the Justice Department and the FBI are trying to force the diversity of services available over the Internet into a single format resembling the telephone network. To do so would irreparably harm the Internet. It would drive up costs for consumers, impair and delay innovation, threaten privacy, and force development of the latest Internet innovations offshore. It is directly contrary to the approach to the Internet

that Congress has wisely pursued for the past decade -- that it remain a relatively unregulated area where new technologies can thrive.

Instead of forcing industry to redesign its products and services to meet government specifications, law enforcement should itself develop the capabilities that it wants to impose on industry. In other words, law enforcement should develop the capability to extract call-identifying information from packet streams. The government will have to develop this capability in-house anyhow, because it will have to be able to deal with sophisticated criminals who can entirely avoid third party service providers and communicate directly and with custom-built protocols. Far and away the most effective approach to Internet interception is for law enforcement to develop the ability to understand Internet communications. Perhaps Congress should appropriate additional funds to the FBI to keep pace with technology and to support state and local law enforcement efforts. Perhaps ways need to be found to draw upon expertise from the private sector. We note that "service bureaus" have come into the market, offering to take on the task of processing digital intercepts.

Rather than demanding that Internet communications be translated into circuit-switched terms, a solution suited to the Internet would probably best be built on the "layered" nature of its architecture. The focus of interception should be at the transport layer, not at the application layer, and the provider of transport services should be obligated only to isolate and deliver to law enforcement the data stream associated with a particular subscriber.

Conclusion

Congress has taken a relatively non-regulatory approach to the Internet and has refrained from applying to the Internet common carriage status and other regulatory burdens applied to telephone companies. CDT has consistently supported this approach. The Internet's rapid growth and innovation attest to the wisdom of this policy. We are now in a time of transition from the narrowband, dial-up Internet of the past to the broadband Internet. The high speed Internet access available via cable modem and digital subscriber lines (DSL) is capable of carrying voice communications of high quality, as well as numerous other applications. This is precisely the wrong time to shoe-horn the Internet into the telecommunications regulatory structure.

CALEA was adopted in 1994 in response to law enforcement concerns that wiretaps would be more difficult in advanced telephone networks. CALEA required telecommunications common carriers to design basic wiretap capabilities into their telephone networks. However, Congress decided in 1994 that CALEA should not apply to the Internet and "information services" carried over it, and rejected FBI proposals that would have gone that far. VoIP, email, Instant Messaging and other forms of Internet communications are information services and thus are not covered by CALEA.

The regulatory framework of CALEA is not suitable for the Internet and Internet applications. The FBI and the Justice Department are absolutely correct when they say that the world of communications has changed dramatically since CALEA was enacted. That is exactly why applying a 10 year old law to this rapidly evolving technology would be a mistake. In sum, expanding CALEA to information services and the Internet would be inappropriate for three reasons:

- It would be unlawful for the FCC to do so – the text of the CALEA excludes broadband Internet access and broadband applications.
- It would be unwise for Congress to do so – CALEA-type mandates would drive up costs, impair and delay innovation, threaten privacy and force development of the latest Internet innovations offshore.
- It would be unnecessary in any event – law enforcement already has Internet surveillance abilities through other statutes and through the cooperation of service providers.